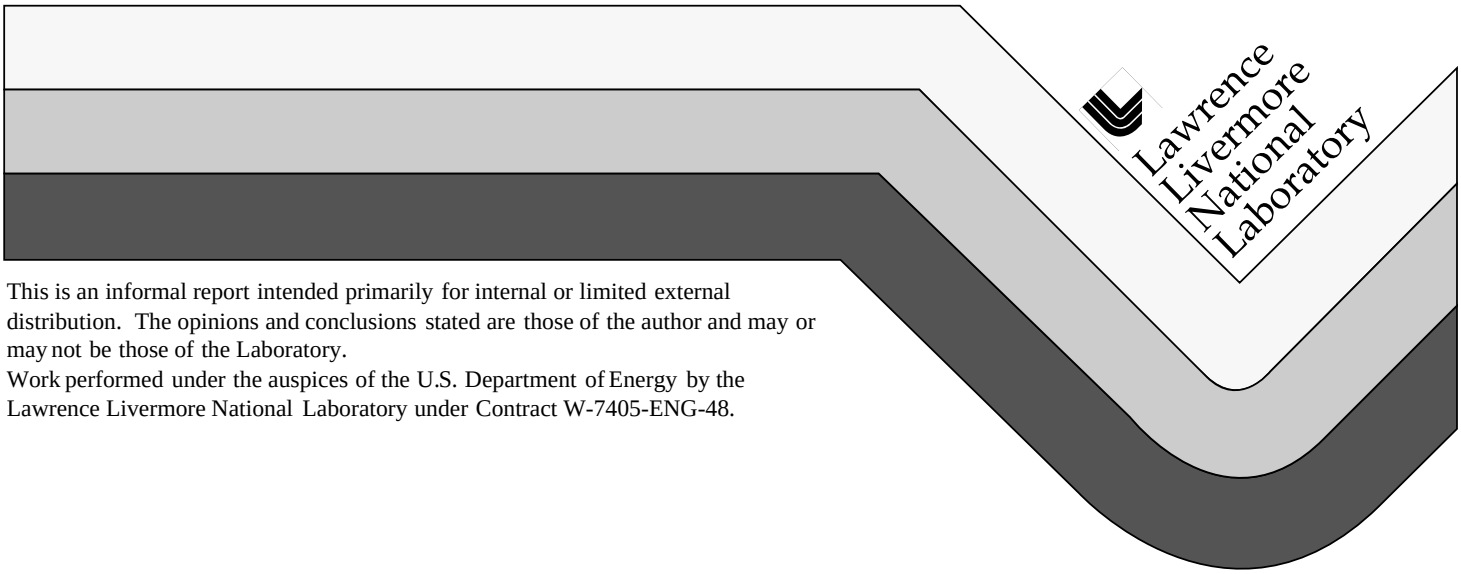
UCRL-ID-132468

Information Warfare Analysis Capability

J. Smart

November 18, 1998



Information Warfare Analysis Capability
J. Smart

With the rapid growth of global computing and communications, information security is a critical issue in all national infrastructure protection discussions. The purpose of our LDRD project-the Information Operations, Warfare, and Assurance (IOWA) initiative-is to advance the enabling core technologies of this field. Special emphasis is placed on computer networks and telecommunication systems. During FY 1998, we developed (1) techniques for identifying the topology of large, complex computer networks, (2) data representation models for these systems, (3) high-performance methods for visualizing the resulting complex models, (4) automated analysis methods for processing large network representations, (5) specialized search techniques for isolating vulnerabilities, (6) a foundation for simulating network operation, and (7) an assessment methodology for determining the consequences of system component failure or disruption.

In order to automate information system protection, it is necessary to first identify the visible components that an intruder might attempt to access and to determine the specific information that might be inferred about each component. We began by developing a set of software modules for analyzing Internet related protocols. This software examines the information that flows across a computer network and extracts network topology and details about each component's configuration. At present, the tool suite processes over twenty popular Internet protocols retrieving over 50 different system operating parameters.

Since modern computer networks have grown considerably in size (i.e. >25,000 nodes), a specially designed model was developed to capture the enormous amount of information that the tools process. The resulting model uses a unique blend of relational database technology integrated into a graph theoretic framework, providing rapid information retrieval in an environment conducive to large network mapping and analysis. A platform-independent viewer for browsing the graph model with integrated access to the relation database was demonstrated. To better manage the complexity of large networks, several powerful dependency constructs, graph operations, and reduction functions were incorporated into the model. A diverse suite of generic graph, fault-tree, and Internet-specific processing algorithms was developed and demonstrated.

To better understand the nature of computer and network vulnerabilities, taxonomy of known vulnerabilities was developed. This taxonomy formed the basis of a new vulnerability database that was constructed. This database was subsequently populated with vulnerability facts from industry and private sources. The end result is a tool that can now be used to automate the search for weaknesses in our computer systems.

Working in unison with the modeling tools, an environment was construct to perform high-fidelity simulations of computer networks. The resulting tools can be used to simulate computer networks captured in the IOWA model. Arbitrary computer networks can also be constructed in the simulation environment and used to generate network traffic to test and calibrate the network mapping tools.